Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

ON THE REAL ELEMENTS OF CERTAIN CLASSES OF GEOMETRICAL CONFIGURATIONS*

By L. E. Dickson

1. The internal structure of many geometrical configurations can be studied best by discussing the related algebraic equations. The nine inflexions of a non-singular plane cubic, the so-called Hessian configuration, give rise to an equation of the ninth degree for their abscissas (or ordinates). So the 27 straight lines on a cubic surface and the 28 bitangents to a plane quartic curve can be found by solving equations of degrees 27 and 28, respectively, for certain parameters. To these and to many other such problems, the theory of groups has been applied by M. Camille Jordan,† for the purpose of showing the precise algebraic character of the solution required in each case, *i. e.*, to show the simplest chain of resolvent equations for each problem.

For the class of problems amenable to statement in terms of abelian functions, a class including five of Jordan's special problems, a general theory was constructed by M. Edmond Maillet in his recent elaborate memoir.‡ The elements of the configuration may be designated by a letter whose subscripts are integers taken modulo r. Maillet's discussion is unnecessarily long and complicated, and restricts§ the modulus r to be a power of a prime. In §3 of the present paper, I give a very simple and direct proof of the general theorem with no restriction whatever upon r.

In his application of the theory of groups to geometrical problems, Jordan was concerned only with the difficulties inherent in the actual determination of the elements of the configuration; he therefore analyzed the equivalent algebraic equation into its resolvents. Maillet makes a noteworthy advance — and this is the most important part of his memoir — by applying group theory to the question of the number of real elements in the configuration. Here also

---

*Read before the American Mathematical Society (Chicago), April 22, 1905.

† *Traité des Substitutions*, pp. 301–369. *Cf.* Dickson, *Linear Groups*, p. 303, *Trans. Amer. Math. Soc.*, vol. 3 (1902), p. 38, and p. 377.

‡ Sur les équations de la géométrie et la théorie des substitutions entre n lettres, *Annales de Toulouse*, (2), vol. 6 (1904), pp. 277–349.

§ Except in a single special case $r = 6$, $r_1 = 3$, $q = 2$, treated on pp. 324–327.

I show how Maillet's long computations can be greatly abridged and his restriction on the modulus r removed (§5). Maillet treats as an isolated problem the question of the reality of the 27 straight lines on a cubic surface, and then deduces an incomplete result on the reality of the 28 bitangents to a quartic curve. Attacking these problems in the reverse order (§§ 7, 8), I obtain results in complete accord with well-known geometrical investigations. Finally, I solve by the same simple method (§§ 6, 9–12) a general class of problems of which this of the 28 bitangents is the lowest special case, the results agreeing with those obtained by Klein by advanced theory of functions.

2. As an illustration of the very general theorem of §3, consider Hesse's configuration of the 9 points of inflexion of a non-singular plane cubic. They lie in sets of 3 on 12 straight lines, each point lying on exactly 4 of the lines. We denote the 9 points by the symbols (xy), in which the indices x, y are integers taken modulo 3. We represent by $(x'y')(x''y'')(x'''y''')$ the inflexional line passing through the points $(x'y')$, $(x''y'')$, and $(x'''y''')$. The 12 inflexional lines correspond to the 12 terms of the function

$$\begin{aligned}\phi = {} & (00)(01)(02) + (00)(10)(20) + (00)(11)(22) + (00)(12)(21) \\ & + (01)(11)(21) + (01)(20)(12) + (01)(10)(22) + (10)(11)(12) \\ & + (02)(12)(22) + (02)(10)(21) + (02)(20)(11) + (20)(21)(22),\end{aligned}$$

in which occur all terms $(x'y')(x''y'')(x'''y''')$ such that

$$x' + x'' + x''' \equiv 0, \quad y' + y'' + y''' \equiv 0 \qquad (\text{mod } 3).$$

A substitution on the 9 symbols (xy) leaves ϕ unaltered if and only if it permutes the indices linearly:*

$$x^* \equiv ax + by + c, \quad y^* \equiv Ax + By + C \qquad (\text{mod } 3).$$

Instead of ϕ, Maillet would employ $\phi + \psi$, where

$$\psi = (00)^3 + (01)^3 + (02)^3 + (10)^3 + (11)^3 + (12)^3 + (20)^3 + (21)^3 + (22)^3$$

involves the 9 inflexional tangents. Our congruence conditions are, in fact, satisfied when $x' \equiv x'' \equiv x'''$, $y' \equiv y'' \equiv y'''$ (mod 3).

While here the addition of the function ψ is trivial since ψ is symmetric, in general the use of all terms whose factors are distinct or not will prove an essential and effective modification of Jordan's use of distinct factors only.

---

* Jordan, *Traité des substitutions*, pp. 302–303.

3. THEOREM. *Let r, r_1, q be any given integers, $r_1 > 2$. With r^q symbols $(x_\rho) = (x_1, x_2, \cdots, x_q)$, the indices x_ρ being integers taken modulo r, form the sum Σ of all the distinct products $(x'_\rho)(x''_\rho)\cdots(x_\rho^{(r_1)})$ such that*

$$(1) \qquad x'_\rho + x''_\rho + \cdots + x_\rho^{(r_1)} \equiv 0 \pmod{r} \qquad (\rho = 1, \cdots, q),$$

repetition of symbols in a product being allowed. The group of all substitutions on the r^q symbols which leave Σ unaltered may be expressed as a linear congruence group Γ on the indices x. Γ contains all the linear homogeneous substitutions

$$(2) \qquad x_i^* \equiv \sum_{j=1}^{q} \xi_{ij} x_j \pmod{r} \qquad (i = 1, \cdots, q),$$

the ξ's being any integers such that $|\xi_{ij}| \not\equiv 0 \pmod{r}$. Also, Γ contains

$$(3) \qquad x_i^* \equiv x_i + a_i \pmod{r} \qquad (i = 1, \cdots, q),$$

where each a_i is a multiple of r/δ, δ denoting the greatest common divisor of r and r_1. Finally, Γ is generated by the substitutions (2) and (3).

To show that substitutions (2) and (3) leave Σ unaltered, it suffices to prove that, when (1) hold, also

$$(1^*) \qquad x_\rho^{*\prime} + x_\rho^{*\prime\prime} + \cdots + x_\rho^{*(r_1)} \equiv 0 \pmod{r} \quad (\rho = 1, \cdots, q).$$

Denote the left members of (1) and (1*) by X_ρ and X_ρ^*. Under (3), $X_\rho^* \equiv X_\rho + r_1 a_\rho \equiv 0 \pmod{r}$, since $r_1 a_\rho$ is a multiple of $r_1 r/\delta$ and hence of r. Under (2),

$$X_\rho^* = \sum_{k=1}^{r_1} x_\rho^{*(k)} \equiv \sum_{k=1}^{r_1} \sum_{j=1}^{q} \xi_{\rho j} x_j^{(k)} = \sum_{j=1}^{q} \xi_{\rho j} \left(\sum_{k=1}^{r_1} x_j^{(k)} \right) = \sum_{j=1}^{q} \xi_{\rho j} X_j \equiv 0.$$

We proceed to the more difficult part of the theorem and prove that every substitution S of Γ can be derived from the types (2) and (3).

Evidently the terms in Σ which are products of r_1 equal symbols are permuted amongst themselves by S; for them

$$(4) \qquad r_1 x'_\rho \equiv 0 \pmod{r}, \quad \frac{r_1}{\delta} x'_\rho \equiv 0 \left(\bmod \frac{r}{\delta}\right), \qquad (\rho = 1, \cdots, q).$$

Hence S replaces the symbol $(0, 0, \cdots, 0)$, which satisfies (4), by a symbol $(x'_1, \cdots, x'_q)$ for which each $x'_\rho \equiv 0 \pmod{r/\delta}$. But there exists a substitution L of the form (3) having this property. Hence $S_0 = SL^{-1}$ leaves fixed

$(0, 0, \cdots, 0) = (0)$. Now S_0 must permute the terms of Σ in which $r_1 - 3$ or more factors are (0), and consequently permutes the products

$$(5) \qquad (x'_\rho)(x''_\rho)(x'''_\rho), \qquad x'_\rho + x''_\rho + x'''_\rho \equiv 0 \pmod{r} \quad (\rho = 1, \cdots, q).$$

Denote by $(\xi_{1i}, \xi_{2i}, \cdots, \xi_{qi})$ the symbol by which S_0 replaces the symbol $u_i = (0, 0, \cdots, x_i = 1, 0, \cdots, 0)$. Among the products (5) occurs $u_1 v_1 (0)$, where $v_1 = (-1, 0, \cdots, 0)$. Hence S_0 replaces v_1 by $(-\xi_{11}, \cdots, -\xi_{q1})$. Again, $v_1 v_1 v_2$ is a product (5) if $v_2 = (2, 0, \cdots, 0)$. Hence S_0 replaces v_2 by $(2\xi_{11}, \cdots, 2\xi_{q1})$, and hence replaces $w_2 = (-2, 0, \cdots, 0)$ by $(-2\xi_{11}, \cdots, -2\xi_{q1})$. Using $v_1 w_2 v_3$, where $v_3 = (3, 0, \cdots, 0)$, we find that S_0 replaces v_3 by $(3\xi_{11}, \cdots, 3\xi_{q1})$. Proceeding by induction, we find that S_0 replaces $(x_1, 0, \cdots, 0)$ by $(x_1\xi_{11}, \cdots, x_1\xi_{q1})$. Similarly, S replaces $(0, \cdots, 0, x_i, 0, \cdots, 0)$ by $(x_i\xi_{1i}, \cdots, x_i\xi_{qi})$. Among the products (5) occurs

$$(-x_1, 0, 0, \cdots, 0)(0, -x_2, 0, \cdots, 0)(x_1, x_2, 0, \cdots, 0).$$

Hence, in view of the previous results, S_0 replaces $(x_1, x_2, 0, \cdots, 0)$, by $(\sigma_1, \cdots, \sigma_q)$, where $\sigma_i = x_1\xi_{i1} + x_2\xi_{i2}$ $(i = 1, \cdots, q)$. Among the products (5) occurs

$$(-x_1, -x_2, 0, 0, \cdots, 0)(0, 0, -x_3, 0, \cdots, 0)(x_1, x_2, x_3, 0, \cdots, 0).$$

Hence S_0 replaces $(x_1, x_2, x_3, 0, \cdots, 0)$ by $(\lambda_1, \cdots, \lambda_q)$, where $\lambda_i = x_1\xi_{i1} + x_2\xi_{i2} + x_3\xi_{i3}$. By induction, we find that S_0 replaces $(x_1, \cdots, x_q)$ by $(x_1^*, \cdots, x_q^*)$, where x_i^* is given by (2).

4. THEOREM.* *If an algebraic equation with distinct roots and with coefficients in a real realm of rationality R has exactly 2ν imaginary roots $x_1, \cdots, x_{2\nu}$ (x_{2j-1} and x_{2j} being conjugates), its Galois group for R contains the substitution*

$$S = (x_1x_2) \cdots (x_{2j-1}\, x_{2j}) \cdots (x_{2\nu-1}\, x_{2\nu}).$$

It suffices† to show that S leaves numerically unaltered every rational

* Maillet's less precise formulation has the restriction that the equation is irreducible. As a generalization, consider an equation $f(x) = 0$ with coefficients in a realm R, not completely solvable in a certain realm R' containing R, but completely solvable in $R'(\rho_1)$, where ρ_1 is a root of a uniserial abelian equation of prime degree p (viz., irreducible in R' with roots $\rho_1, \Theta(\rho), \Theta^2(\rho_1), \ldots$); then the Galois group of $f(x)$ for R contains the substitution $(x_1x_2 \ldots x_p)(x_{p+1} \ldots x_{2p}) \ldots (x_{\nu p-p+1} \ldots x_{\nu p})$, if $x_1, \ldots, x_{\nu p}$ are the roots in $R'(\rho_1)$ but not in R'.

†See, for example, Dickson's *Algebraic Equations*, bottom of p. 54, for $G'' = \{1, S\}$.

function $\varphi(x_1, \cdots, x_n)$ of the roots such that φ has its coefficients in R and equals a quantity in R. The numerical value of φ being real, φ remains numerically unaltered when $i = \sqrt{-1}$ is changed into $-i$ in each imaginary root; but the resulting change in φ is equivalent to the application of the substitution S.

COROLLARY. *Either the roots are all real or their number is the number of letters unaltered by one of the substitutions of period 2 of the Galois group.*

5. THEOREM. *The number of symbols $(x_1, \cdots, x_q)$ unaltered by a q-ary linear homogeneous substitution modulo r is a divisor of r^q. For a non-homogeneous substitution, the number is 0 or a divisor of r^q.*

The conditions that $x_i^* \equiv x_i$ in (2) are q homogeneous linear congruences

$$(2') \qquad x_i \equiv \sum_{j=1}^{q} \xi_{ij} x_j \pmod{r} \qquad (i = 1, \cdots, q).$$

The number of incongruent sets of solutions $x_1, \cdots, x_q$ is known* to be a divisor d of r^q. Next, if there be one set of solutions $x_1', \cdots, x_q'$ of the non-homogeneous congruences

$$x_i \equiv \sum_{j=1}^{q} \xi_{ij} x_j + \xi_i \pmod{r} \qquad (i = 1, \cdots, q),$$

then the d existing sets of solutions are $x_1 + x_1', \cdots, x_q + x_q'$, where the sets $x_1, \cdots, x_q$ give all the previous sets of solutions of $(2')$.

In view of §§3–4, this theorem gives a set of numbers among which must occur the number of real elements of a geometrical configuration of the extensive class expressible in terms of abelian functions. For some of these configurations, more precise limits for the number of real elements may be given (§§6–12).

6. Some of the most interesting questions in geometry relate to the problems of contact of curves. Certain problems of the kind discussed by Steiner† and Hesse† were treated from a more general standpoint by Clebsch‡ in his paper on the application of abelian functions to geometry. Let C_n be a plane curve of order n having no double points and set $p = \frac{1}{2}(n-1)(n-2)$.

* Bachmann, *Die Arithmetik der Quadratischen Formen*, I, p. 353.

† *Journal für Mathematik*, vol. 49 (1855).

‡ *Ibid*, vol. 63 (1864), pp. 189–243.

Clebsch proved that there are $R_p \equiv 2^{2p-1} - 2^{p-1}$ curves of order $n-3$ having simple contact with C_n at $\frac{1}{2}\, n(n-3)$ points. The determination of these curves depends upon an algebraic equation E of degree R_p whose roots may be symbolized $(x_1y_1 \cdots x_py_p)$ where $x_1, \cdots, y_p$ form a set of solutions of

$$(6) \qquad x_1y_1 + x_2y_2 + \cdots + x_py_p \equiv 1 \pmod 2.$$

Clebsch showed that, if μ is any integer $\gtreqless R_p$ for which $\frac{1}{2}\,\mu(n-3)$ is an integer, the points of contact of C_n with the μ curves corresponding to the roots

$$(7) \qquad (x_1'y_1' \cdots x_p'\, y_p'), \cdots, (x_1^{(\mu)}y_1^{(\mu)} \cdots x_p^{(\mu)}y_p^{(\mu)})$$

lie on a curve of order $\frac{1}{2}\,\mu(n-3)$ if the following congruences hold simultaneously:

$$(8) \quad x_\rho' + x_\rho'' + \cdots + x_\rho^{(\mu)} \equiv 0, \quad y_\rho' + y_\rho'' + \cdots + y_\rho^{(\mu)} \equiv 0 \pmod 2 \quad (i = 1 \cdots, p).$$

Hence the substitutions of the Galois group G of equation E leave invariant the sum ϕ_μ of the products of μ roots (7) satisfying (8). If n be even, μ can have only even values. A substitution leaves invariant $\phi_4, \phi_6, \phi_8, \cdots$, if and only if it has the form*

$$(9) \quad x_i^* = \sum_{j=1}^{p} (\alpha_{ij}x_j + \gamma_{ij}y_j) + \rho_i, \quad y_i^* = \sum_{j=1}^{p} (\beta_{ij}x_j + \delta_{ij}y_j) + \sigma_i \quad (i = 1, \cdots, p),$$

$$(9') \qquad \rho_i \equiv \sum_{j=1}^{p} \alpha_{ij}\gamma_{ij}, \quad \sigma_i \equiv \sum_{j=1}^{p} \beta_{ij}\delta_{ij},$$

the coefficients α, γ, β, δ being subject to the abelian conditions†

$$(10) \qquad \sum_{i=1}^{p} \begin{vmatrix} \alpha_{ki}\gamma_{ki} \\ \alpha_{ji}\gamma_{ji} \end{vmatrix} = 0, \quad \sum_{i=1}^{p} \begin{vmatrix} \beta_{ki}\delta_{ki} \\ \beta_{ji}\delta_{ji} \end{vmatrix} = 0, \quad \sum_{i=1}^{p} \begin{vmatrix} \alpha_{ki}\gamma_{ki} \\ \beta_{ji}\delta_{ji} \end{vmatrix} = \begin{matrix} 0 \ (j \neq k), \\ 1 \ (j = k), \end{matrix}$$

holding for $j, k = 1, \cdots, p$. The group A_{2p} of the substitutions (9) subject to (10) is thus simply isomorphic to the abelian linear homogeneous group on $2p$ indices modulo 2 and leaves invariant $x_1y_1 + \cdots + x_py_p$ modulo 2. Taking $\mu = 3$ in (8) we see at once that (9) will leave $\phi_3, \phi_5, \cdots$, invariant if and only if $\rho_i \equiv \sigma_i \equiv 0 \pmod 2$ for $i = 1, \cdots, p$. Hence‡ the substitutions leaving every ϕ_μ invariant form the first hypoabelian group H_{2p}, modulo 2

* Dickson, *Trans. Amer. Math. Soc.*, vol. 3 (1902), pp. 377–382.

† In the present special case, conditions (10) are congruences modulo 2.

‡ This immediate proof may be contrasted with the very complicated proof by Jordan, *Traité*, pp. 242–249, and with the writer's simplification, *Transactions*, vol. 3 (1902), pp. 38–45.

(usually defined as the largest linear homogeneous group leaving $x_1y_1 + \cdots + x_py_p$ invariant modulo 2).

7. For $n = 4$, we have $p = 3$, $R_p = 28$, so that the problem is that of the 28 bitangents to a quartic curve without double points. In the abelian group on 6 indices modulo 2, every operator of period 2 is conjugate* with M_1, M_1M_2, $M_1M_2M_3$ or R_{121}, where

$$(11) \qquad M_i\colon\ x_i' = y_i,\quad y_i' = -x_i;\ R_{ij\lambda}\colon\ y_i' = y_i - \lambda x_j,\quad y_j' = y_j - \lambda x_i.$$

This result will be established directly in §11. These substitutions (11) correspond to themselves in the group A_6 since for them $\rho_i \equiv \sigma_i \equiv 0$. Of the 28 symbols $(x_1y_1\ x_2y_2\ x_3y_3)$ for which $x_1y_1 + x_2y_2 + x_3y_3 \equiv 1 \pmod 2$, M_1 leaves fixed the 16 symbols with $x_1 \equiv y_1$, R_{121} leaves fixed the 4 symbols with $x_1 \equiv x_2 \equiv 0$, $x_3 \equiv y_3 \equiv 1$. Similarly, M_1M_2 leaves fixed 8 symbols; $M_1M_2M_3$, 4 symbols. Applying the corollary of §4, we have the

THEOREM. *Of the* 28 *bitangents to a real quartic curve without double points, exactly* 4, 8, 16, *or* 28 *are real.*†

8. A mutual connection‡ exists between the 28 bitangents to a quartic curve and the 27 straight lines on a general cubic surface S. From any point P of S can be drawn a quartic cone C touching S. The bitangent planes of C are the 27 planes joining P with the 27 lines on S, and the tangent plane to S at P. An arbitrary plane cuts C and its bitangent planes in a quartic curve and its 28 bitangents. We can proceed inversely by projection.

If to the domain of rationality we adjoin one root of the equation for the 28 bitangents, the Galois group reduces to a group simply isomorphic with the Galois group of the 27 straight lines on the cubic surface.§ Hence we have the

THEOREM. *Of the* 27 *straight lines on a general real cubic surface, exactly* 3, 7, 15, *or* 27 *are real.*‖

---

* Dickson, *American Journal of Mathematics*, vol. 26 (1904), p. 318.

† Zeuthen, *Mathematische Annalen*, vol. 7 (1873), p. 411; Salmon's *Higher Plane Curves*, p. 220; Weber's *Algebra*, II. That no other than these four cases can occur requires an eight page discussion by Weber; that the four cases all actually occur is proved more easily. Maillet's group discussion (*l. c.* p. 323) is incomplete as it fails to exclude the case of no real bitangents.

‡ Geiser, *Mathematische Annalen*, vol. 1 (1869), pp. 129–138.

§ Jordan, *Traité des substitutions*, p. 330.

‖ That these four, but no other, cases arise was shown by Schläfli, *Quarterly Journal of Mathematics*, vol. 2 (1858), pp. 110–120; particularly p. 117. The complete theorem is not given by d'Ocagne and Lévy, to whom Maillet refers exclusively.

9. For application to the contact problems in §6 and to various questions in abelian functions, we determine representatives of each set of conjugate operators of period 2 in the special abelian group $SA(2p, q^n)$ of all linear transformations

$$S: \quad x_i' = \sum_{j=1}^{p} (a_{ij}\, x_j + \gamma_{ij}\, y_j),\ y_i' = \sum_{j=1}^{p} (\beta_{ij}\, x_j + \delta_{ij}\, y_j) \quad (i = 1, \cdots, p),$$

with coefficients in the Galois field of order q^n which satisfy relations (10). If S is of period 2, all the roots of its characteristic equation are ± 1 and there is a linear function f which S multiplies by $\epsilon_1 = \pm 1$. There exists an abelian substitution which replaces x_1 by f, and hence transforms S into S', which replaces x_1 by $\epsilon_1\, x_1$. Then by (10),

$$\delta_{11} = \epsilon_1,\ \gamma_{i1} = \delta_{i1} = 0 \qquad (i = 2, \cdots, p),$$

while a_{ij}, γ_{ij}, β_{ij}, δ_{ij} $(i, j = 2, \cdots, p)$ define an abelian transformation Σ on $x_2, y_2, \cdots, x_p, y_p$. Since $S'^2 = I$, the identity, we have $\Sigma^2 = I$.

We employ below the simple abelian substitutions (11) and

$$T_{i,\lambda}:\ x_i' = \lambda x_i,\ y_i' = \lambda^{-1} y_i\,; \quad L_{i,\lambda}':\ y_i' = y_i + \lambda x_i\,;$$

$$Q_{i,j,\lambda}:\ x_i' = x_i + \lambda x_j,\ y_j' = y_j - \lambda y_i$$

10. THEOREM.* *If $q > 2$, every operator of period 2 of $SA(2p, q^n)$ is conjugate with $T_{1,-1}$, $T_{1,-1}\, T_{2,-1}$, $\cdots$, or $T_{1,-1}\, T_{2,-1} \cdots T_{p,-1}$.*

We assume that the theorem is true for $p - 1$ pairs of variables and prove it true for p pairs. Hence we may set $\Sigma = T_{2,\epsilon_2} \cdots T_{p,\epsilon_p}$, each $\epsilon^2 = 1$. Then S', being of period 2, becomes S'':

$$x_1' = \epsilon_1 x_1, \qquad y_1' = \epsilon_1 y_1 + \sum_{j=2}^{p} (\beta_{1j}\, x_j + \delta_{1j} y_j),$$

$$x_i = \epsilon_i x_i + \delta_{1i} x_1, \qquad y_i' = \epsilon_i\, y_i - \beta_{1i}\, x_1 \qquad (i = 2, \cdots, p),$$

in which by (10), $(\epsilon_1 + \epsilon_i)\delta_{1i} = 0$, $(\epsilon_1 + \epsilon_i)\, \beta_{1i} = 0$. If $\delta_{12} = 0$, $\beta_{12} = 0$, $(x_1 x_2)\,(y_1 y_2)$ transforms S'' into $T_{1,\epsilon_2}'\, T$, where T is abelian on x_i, y_i $(i > 1)$, so that the theorem follows. If δ_{12}, β_{12} are not both zero, so that $\epsilon_2 = -\epsilon_1$, we may set $\delta_{12} \neq 0$ (transforming by M_2 in the contrary case), and make $\beta_{12} = 0$ (by transforming by $L_{2,\rho}'$). Transforming by $Q_{2,1,\lambda}$, $\lambda = -\frac{1}{2}\epsilon_1 \delta_{12}$, we obtain a substitution of the form S'' with $\beta_{12} = \delta_{12} = 0$, a case just treated. The theorem is evident for S' when $p = 1$.

---

* *Linear Groups*, pp. 100–105. The present proof is incomparably simpler.

11. THEOREM. *If $q = 2$, every operator of period 2 of $SA(2p, q^n)$ is conjugate with $L'_{1,1}$, $L'_{1,1}L'_{2,1}, \cdots, L'_{1,1}L'_{2,1} \cdots L'_{p,1}$, $R_{1,2,1}$, $R_{1,2,1}R_{3,4,1}, \cdots$, or $R_{1,2,1}R_{3,4,1} \cdots R_{2\pi-1,2\pi,1}$ where π is the greatest integer in $p/2$.*

We proceed by induction from $p-1$ to p pairs of variables. The theorem is true for $p = 1$, since S' is then $L'_{1,\beta_{11}}$, which is transformed into $L'_{1,1}$ by $T_{1,\beta_{11}^{1/2}}$. For $p > 1$, we can by hypothesis give to Σ (of §9) one of the following forms:

(*a*) $\Sigma = R_{2,3,1}R_{4,5,1} \cdots R_{2k,2k+1,1}$. Then S' being abelian and of period 2 becomes

$$x'_1 = x_1, \quad y'_1 = y_1 + \sum_{j=1}^{p} \beta_{1j}x_j + \sum_{j=2k+2}^{p} \delta_{1j}y_j,$$

$$x'_2 = x_2, \quad y'_2 = \beta_{12}\, x_1 + y_2 + x_3,\ x'_3 = x_3,\ y'_3 = \beta_{13}\, x_1 + x_2 + y_3, \cdots.$$

Its transform by $Q_{2,1,\beta_{13}}\, Q_{3,1,\beta_{12}}$ is S_1, of the form S' with $\beta_{12} = \beta_{13} = 0$. Hence $(x_1x_2x_3)\,(y_1y_2y_3)$ transforms S_1 into $R_{1,2,1}T$, T being abelian on $x_i, y_i (i > 2)$. To T we apply the hypothesis for the induction. But

$$x'_1 = x_1 + x_3,\ x'_2 = x_2 + x_3,\ x'_3 = x_1 + x_2 + x_3,\ y'_1 = y_2 + y_3,\ y'_2 = y_1 + y_3,$$
$$y'_3 = y_1 + y_2 + y_3$$

is abelian and transforms $R_{1,2,1}\, L'_{3,1}$ into $L'_{1,1}\, L'_{2,1}\, L'_{3,1}$. Hence $R_{1,2,1}T$ is conjugate with a product of the L''s or with a product of the R's.

(*b*) $\Sigma = L'_{2,1}\, L'_{3,1} \cdots L'_{r,1}$. Then S' becomes

$$x'_i = x_i\ (i = 1, \cdots, r),\ y'_1 = y_1 + \sum_{j=1}^{p} \beta_{1j}x_j + \sum_{j=r+1}^{p} \delta_{1j}y_j,$$

$$y'_i = \beta_{1i}x_1 + x_i + y_i\ (i = 2, \cdots, r),\ x'_k = \delta_{1k}x_1 + x_k,\ y'_k = \beta_{1k}x_1 + y_k\ (k > r).$$

Its transform by $Q_{2,1,\beta_{12}}$ is of like form with $\beta_{12} = 0$. Transforming the result by $(x_1x_2)\,(y_1y_2)$, we get $L'_{1,1}T$, T being abelian on x_i, y_i $(i > 1)$. As at the end of case (*a*) we reach a product of the L''s.

(*c*) $\Sigma =$ identity. Then S', being of period 2, is

$$x'_1 = x_1,\ y'_1 = y_1 + \sum_{j=1}^{p} \beta_{1j}x_j + \sum_{j=2}^{p} \delta_{1j}y_j,\ x'_i = x_i + \delta_{1i}x_1,\ y'_i = y_i + \beta_{1i}x_1\ (i > 1).$$

If $\beta_{1j} = \delta_{1j} = 0\ (j = 2, \cdots, p)$, $S' = L'_{1,\beta_{11}}$. In the contrary case, we apply an abelian transformation on $x_2, \cdots, y_p$ and make $\beta_{12} = 1$, $\delta_{12} = 0$, $\beta_{1i} = \delta_{1i} = 0\ (i > 2)$, obtaining $L'_{1,\beta}\, R_{1,2,1}$. If $\beta \neq 0$, we transform by $Q_{1,2,\beta^{-1}}$ and reach $L'_{1,\beta}L'_{2,\beta^{-1}}$.

Since $x_1' = x_1 + y_1$ transforms $L_{1,1}'$ into $M_1 = (x_1y_1)$, we obtain the

COROLLARY. *The operators of period 2 of $SA(2p, 2^n)$ are conjugate with $M_1, M_1M_2, \cdots, M_1M_2 \cdots M_p, R_{1,2,1}, R_{1,2,1}R_{3,4,1}, \cdots$, or $R_{1,2,1}R_{3,4,1} \cdots R_{2\pi-1,2\pi,1}$.*

12. We can now generalize the results of §7 on the 28 bitangents to a quartic curve. A symbol $(x_1y_1 \cdots x_py_p)$ is unaltered by $R_{1,2,1}R_{3,4,1} \cdots R_{2k-1,2k,1}$ if and only if $x_i \equiv 0 \pmod 2$, for $i = 1, \cdots, 2k$, so that the number of unaltered symbols is $2^{2k}R_{p-2k}$. Next, $M_1M_2 \cdots M_k$, $k \gtrless p$, leaves unaltered only the symbols with $x_i \equiv y_i$ $(i = 1, \cdots, k)$, their number being 2^{2p-1-k} since $\sum_{i=1}^{k} x_i^2 + \sum_{i=k+1}^{p} x_iy_i \equiv 1 \pmod 2$ uniquely determines $x_1 \pmod 2$, in terms of the other $2(p-k) + k - 1$ variables entering. In view of the corollary in §11, we derive the

THEOREM. *Any operator of period 2 of the Steiner group A_{2p} of §6 leaves fixed exactly $2^{2p-2k-1} - 2^{p-1}$ $(k = 1, \cdots, \pi)$ or 2^{2p-1-k} $(k = 1, \cdots, p)$ symbols, where π is the greatest integer in $p/2$.*

Remark. This theorem holds *a fortiori* for the subgroup H_{2p} of §6 on the same R_p symbols. It is important to notice that all the cases for A_{2p} occur for H_{2p} since $M_1, \cdots, M_1M_2 \cdots M_p$, and $R_{1,2,1}, \cdots$ belong* to H_{2p}.

In view of §§4, 6, we may now state the

THEOREM. *Let C_n be a real curve of order n having no double points and set $p = \frac{1}{2}(n-1)(n-2)$. Of the $2^{2p-1} - 2^{p-1}$ curves of order $n-3$ having simple contact with C_n at $\frac{1}{2}n(n-3)$ points, either all or $2^{2p-2k-1} - 2^{p-1}$ $(k = 1, \cdots, \pi)$ or 2^{2p-1-k} $(k = 1, \cdots, p)$ are real, where $\pi = p/2$ or $(p-1)/2$.*†

Besides the case of the 28 bitangents to a quartic, we note that *of the* 2016 *conics tangent at* 5 *points to a quintic curve* (*without double points*), *either* 2016, 1024, 512, 480, 256, 128, 96, 64, 32, *or none are real.*

THE UNIVERSITY OF CHICAGO,
FEBRUARY, 1905.

---

* Whether or not the Corollary in §11 holds true for the first hypoabelian group on $2p$ variables in the $GF[2^n]$ remains undecided. I have proved it true for $p = 1$ or 2.

† This result is in complete accord with that by Klein, *Math. Ann.*, vol. 42 (1893), pp. 26–27; the different ranges of values for λ being given on p. 3. For details, see Klein's *Riemann'sche Flächen*, II (1892), pp. 117–255.